

UNITED STATES DISTRICT COURT
DISTRICT OF NEVADA

UNITED STATES OF AMERICA,

Plaintiff,

vs.

CHAD ASKREN,

Defendants.

Case No. 2:14-cr-314-GMN-GWF

**FINDINGS &
RECOMMENDATIONS**

Motion to Suppress (#16)

This matter is before the Court on Defendant Chad Askren's Motion to Suppress Evidence (#16), filed on April 28, 2015. The Government filed its Response (#23) on June 5, 2015 and Defendant filed his Reply (#26) on June 10, 2015. The hearing on the motion to suppress was continued at the request of the parties and was conducted by the Court on September 10, 2015.

BACKGROUND

The indictment in this case charges Defendant Chad Askren with receipt of child pornography in violation of 18 U.S.C. § 2252A(a)(2) and (b); possession of child pornography in violation of 18 U.S.C. § 2252A(a)(5)(B) and (b); and advertising child pornography in violation of 18 U.S.C. § 2251(d). These charges arise from evidence allegedly discovered during the December 13, 2012 search of a residence located at 514 Crimson View Place, Las Vegas, Nevada, 89144. The search was conducted pursuant to a warrant issued by the undersigned magistrate judge on December 10, 2012. During the search, a computer allegedly belonging to Defendant Askren was seized. A forensic examination of the computer resulted in the discovery of 76 videos and 5,284 images depicting child pornography.

...

1 The search warrant was based on an affidavit by William C. Hedges, a Special Agent (SA)
2 of the Department of Homeland Security, Homeland Security Investigations (HSI) (hereinafter
3 “Agent Hedges”). *See Motion (#16), Search Warrant Affidavit, Exhibit 1; Government’s Response,*
4 *Exhibit A (hereinafter “Affidavit”).* Agent Hedges stated in his affidavit that as part of his daily
5 duties, he investigates criminal violations relating to child exploitation and child pornography. He
6 has received training in the areas of child pornography and child exploitation; conducted and
7 assisted in the execution of Federal child pornography search warrants; and conducted and assisted
8 in the seizure of computers and media storage devices containing child pornography. *Affidavit*, ¶ 1.
9 The affidavit contained a recitation of the child pornography criminal statutes, ¶¶ 5-10; definitions
10 of terms relating to child pornography laws, computers, digital devices, and the internet, ¶ 11(a)-(t);
11 a background on computers and child pornography, and online child exploitation, including the
12 behavioral characteristics of “people who produce, trade, distribute, or possess images of child
13 pornography” and the manner in which computers and the internet are used to facilitate these
14 activities, ¶¶ 12-21; the manner in which searches of computers are conducted, ¶¶ 22-24; and the
15 search methodology to be employed in searching the hard drive of a computer(s) for evidence of
16 child pornography or evidence of other criminal activity that may be stored on a computer hard
17 drive. ¶ 25(a)-(h).

18 The affidavit also provided the following “Background on Node-to-Node File Sharing:”

19 26. An increasingly common activity on the Internet is
20 peer-to-peer (P2P) file sharing. P2P file sharing is a method of
21 communication available to Internet users through the use of special
22 software. Computers link together through the Internet using this
23 software form a network that allows for the sharing of digital files
24 between users on the network. A user first obtains the P2P software,
25 which can be downloaded from the Internet. In general, P2P software
26 allows the user to set up file(s) on a computer to be shared with others
27 running compatible P2P software. A user obtains files by opening the
28 P2P software on the user’s computer, and conducting a search for files
that are currently being shared on the network. One of the newest
evolutions of P2P software allows users to setup their own private
P2P network of contacts. File sharing through these new and publicly
available P2P file sharing programs is limited to only other users who
have been added to a user’s private list of “friends.” A new user is
added to your list of friends through a friend request. Acceptance of a
friend request will allow the new user to browse the list of files that
the other user who sent the friend request has made available. The
new user can then select the file(s) from this list and download the

1 selected file(s). Whether by using a friend-list version of the software
2 or by one that allows all users to see the files available, the download
3 of a file is achieved through a direct connection between the computer
4 requesting the file and the computer containing the file.

5 27. One of the advantages of some P2P file-sharing
6 programs is that multiple files may be downloaded in parallel. This
7 means that the user can download more than one file at a time.
8 However, this feature was not enabled in this investigation. The files
9 downloaded were from a single source.

10 28. A P2P file transfer is assisted by reference to an
11 Internet Protocol (IP) address. The IP address provides a unique
12 location making it possible for data to be transferred between
13 computers.

14 29. Third-party software, such as CommView, can be
15 loaded on a computer and used to monitor and log Internet traffic
16 between two computers. Such software enables its user to identify the
17 IP address of the P2P computer containing the file, and to identify if
18 parts of the file came from one or more IP addresses. Such software
19 further monitors and logs Internet and local network traffic.

20 30. The computers that are linked together to form a P2P
21 network are located throughout the world; therefore, the P2P network
22 operates in interstate and foreign commerce. A person who includes
23 child pornography files in his/her "shared" folder is hosting child
24 pornography and is thereby promoting, presenting, and potentially
25 distributing child pornography. A person who hosts child
26 pornography in this fashion is in violation of Title 18, United States
27 Code, Section 2252A(a)(3)(B) in that he/she is promoting and
28 presenting child pornography in interstate and foreign commerce by
means of a computer.

31. Even though P2P networks link together computers all
over the world and users can download files, it is not possible for one
user to send or upload a file to another user through the P2P network.
The software is designed only to allow files to be downloaded that
have been selected. One does not have the ability to send files from
his/her computer to another user's computer or to download files from
another user's computer without the other user's permission,
knowledge, and active participation.

Affidavit, ¶¶ 26-31.

Under "Details of Investigation," Agent Hedges stated that he initiated an online undercover
investigation on October 2, 2012. Using law enforcement computer software, Agent Hedges
identified a computer located at Internet Protocol (IP) address 68.229.54.147 as having numerous
file names indicative of child pornography available to be shared on the ARES P2P Network.

Affidavit, ¶ 32. The ARES P2P Network is a de-centralized file sharing network that uses the

1 Internet. Using ARES Galaxy software, users can download and share images, videos, music, etc.
2 The data to be shared is stored on each ARES Galaxy user's computer and allowed to be shared, or
3 not to be shared by the user. ¶ 33. The affidavit further stated:

4 34. To share files on the ARES network, the user has to
5 search for and download a software application capable of interfacing
6 with the ARES network. This application, when installed, allows the
7 user to search for pictures, movies or other digital files using search
8 terms. A text search goes to a "Supernode," an index server that
9 handles requests and examines submitted file lists from a "node"
10 (other individual ARES network participant users) that it knows about
11 for files matching the text search request. A file list is then sent back
12 to the requesting user who can choose to download files from a node
13 that possesses at least a portion of the files. For files to be shared on
14 the ARES network, the individual user's application must be set up to
15 identify files and folders available for sharing. The application will
16 then proceed to make available any file the user chooses to share.
17 Your affiant knows from training and experience that search results
18 presented to the user allow the user an option to select (or not to
19 select) a file and then to take additional steps to download the file to
20 their own computer. During this process, parts of the downloaded file
21 can be received from other users around the world. Because users can
22 receive parts of the selected file from numerous sources
23 simultaneously, downloading files from peers is much faster than
24 downloading a file from a single source.

25 35. Your affiant knows that the files shared by the users of
26 the ARES network are identified by a file name and mathematical
27 algorithm known as Secure Hash Algorithm Version 1, or SHA-1,
28 hash value. While file names are more intuitive to a human being
when searching for content and selecting files for download, the
actual uniqueness of each file is identified by its SHA-1, hash value,
which the ARES network uses to index files. SHA-1, hash values are
a long string of alpha numeric characters to represent the data in the
shared file. SHA-1 was developed by the National Institute of
Standards and Technology (NIST), along with the National Security
Agency (NSA). The United States of America has adopted the SHA-
1, hash algorithm as a Federal Information Processing Standard. It is
computationally infeasible . . . to find two different files that produce
the same SHA-1, hash value. This allows investigators to identify a
file by the value, regardless of the name of the file, with greater than
99.99 percent certainty. The SHA-1 digital signature can be explained
as a digital fingerprint, or DNA of the file. Your affiant has been
trained, and is able to compare the SHA-1 digital fingerprint value of
files being shared on the network to previously identified SHA-1,
hash values of any file, including child pornography, which are known
to investigators. Your affiant knows that even if a user changes the
file name, the SHA-1, hash value, or digital fingerprint for the file,
will remain the same.

36. The target IP address (68.229.54.147) was identified as
being a "download candidate," offering images depicting child
pornography for sharing numerous times on October 2, 2012. In order

1 to be a download candidate for child sexual exploitation files of
2 investigative interest previously identified, the ARES network
3 software on the subject computer must have reported to the network
4 that it had files available for sharing, that had a SHA-1 hash value that
5 your affiant knows matched the SHA-1 hash values of
known/previously viewed child pornography available for trade
through the network. A computer at the target IP address was
identified and recorded as a download candidate on several occasions
before and after October 2, 2012.

6 *Affidavit*, ¶¶ 34-36.

7 Agent Hedges stated that on October 2, 2012, he used a law enforcement software program
8 to compare SHA-1 values advertised by the computer using IP address 68.229.54.147 to SHA-1
9 values stored in the agent's known child exploitation files library, and "located many files that
10 depict child pornography." *Affidavit*, ¶ 37. On October 2, 2012, Agent Hedges downloaded four
11 files from the computer using IP address 68.229.54.147 that contained images of child pornography.
12 *Id.*, ¶ 38.¹

13 Agent Hedges further stated that a records check revealed that Cox Communications was the
14 owner of IP address 68.229.54.147. On October 16, 2012, a Department of Homeland Security
15 summons was sent to Cox Communications requesting subscriber information for IP address
16 68.229.54.147 for the specific date and time of the suspected activity. Cox Communications
17 responded to the summons on October 19, 2012 and advised that at the requested date and time IP
18 address 68.229.54.147 was assigned to the residential account of an individual who is identified by
19 the parties as "CS"² with a residential address of 514 Crimson View Pl., Las Vegas, Nevada 89144,
20 together with a listed telephone number. A records check with the Nevada Department of Motor
21 Vehicles also listed CS's address as 514 Crimson View Pl., Las Vegas, Nevada 89144. The Clark
22 County Assessors Office listed CS as the owner of the residential property. A records check with
23 Nevada Energy showed that CS was the subscriber for utility service at the residence. Citizen and
24 Immigration Service (CIS) reported that CS is a citizen of Italy and is a Legal Permanent Resident in

26 ¹ Defendant does not dispute that the images described in Agent Hedges' affidavit meet the
27 definition of "child pornography" in 18 U.S.C. § 2256(8).

28 ² CS's full name is stated in Agent Hedge's affidavit.

1 the United States. *Affidavit*, ¶¶ 39-43.

2 Agent Hedges conducted surveillance at 514 Crimson View Place on November 19, 20 and
3 December 4, 2012. No one was seen entering or exiting the residence during this surveillance and
4 no vehicles were observed at the residence. On November 19th and December 4th trash cans were
5 sitting on the curb in front of the residence. *Affidavit*, ¶ 44.

6 The search warrant authorized the law enforcement agents to search 514 Crimson View
7 Place, including any computers found on the premises, for evidence of child pornography. *See*
8 *Affidavit, Attachments A and B*. During the execution of the search warrant, CS told law
9 enforcement agents that he had a wireless network and a password protected router. CS also stated
10 that Defendant Askren was his roommate and had access to the network. *Government's Response*
11 *(#23)*, pg 3:7-9. According to the Government, "[a] preview of the Defendant's computer showed
12 indicia of child pornography." *Id.*, at 3:9-10. Defendant states that CS also told the agents that
13 Defendant had been living with his girlfriend and would only come to CS's home to check his mail.
14 *Motion (#16)*, pg 3:6-7.

15 DISCUSSION

16 Defendant Askren argues that Agent Hedge's affidavit did not provide sufficient facts to
17 support a finding of probable cause to search the premises at 514 Crimson View Place for evidence
18 of child pornography. Defendant also asserts that the information in the affidavit was stale because
19 the agents did not apply for the search warrant until more than two months after Agent Hedges
20 downloaded images of child pornography from the computer using IP address 68.229.54.147.
21 Defendant further argues that the affidavit was so lacking in the indicia of probable cause that
22 agents did not have a good faith basis to rely on the validity of the warrant. The Government
23 disputes each of Defendant's contentions.

24 The Fourth Amendment to the United States Constitution provides that "[t]he right of the
25 people to be secure in their persons, houses, papers, and effects, against unreasonable searches and
26 seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by
27 Oath or affirmation, and particularly describing the place to be searched, and the persons or things to
28 be seized." A search warrant is supported by probable cause if the issuing judge finds that "given

1 all the circumstances set forth in the affidavit before him . . . there is a fair probability that
2 contraband or evidence of a crime will be found in a particular place.” *United States v. Underwood*,
3 725 F.3d 1076, 1081 (9th Cir. 2013), quoting *Illinois v. Gates*, 462 U.S. 213, 238, 103 S.Ct. 2317,
4 76 L.Ed.2d 527 (1983). “Whether there is a fair probability depends on the totality of the
5 circumstances, including reasonable inferences, and is a ‘common sense, practical question.’ . . .
6 Neither certainty nor a preponderance of the evidence is required.” *United States v. Kelley*, 482 F.3d
7 1047, 1050 (9th Cir. 2007), citing *United States v. Gourde*, 440 F.3d 1065, 1069 (9th Cir. 2006) (en
8 banc). “An affidavit must recite underlying facts so that the issuing judge can draw his or her own
9 reasonable inferences and conclusions; it is these facts that form the central basis of the probable
10 cause determination.” *Underwood*, 725 F.3d at 1081. Expert opinion about the behavior of a
11 particular class of persons may also be considered in the totality of the circumstances. The affidavit
12 must, however, lay a foundation which shows that the person subject to the search is a member of
13 the class. *Id.*

14 Probable cause in this case was predicated on Agent Hedges’ downloading of child
15 pornography images from a computer that made them available for downloading on the ARES P2P
16 network on October 2, 2012. The computer that made the images available used IP address
17 68.229.54.147. Through follow-up investigation, Agent Hedges determined that on October 2, 2012
18 IP address 68.229.54.147 was assigned by Cox Communications to the residential account of CS
19 whose address was 514 Crimson View Pl., Las Vegas, Nevada 89144. Further inquiries to the
20 Nevada Department of Motor Vehicles, NV Energy, and Citizen and Immigration Service also
21 indicated that CS resided at 514 Crimson View Place. Subsequent surveillance of the residence did
22 not result in the observation or identification of any individuals or motor vehicles going to or
23 coming from the residence. The presence of trash cans in front of the residence on two of the three
24 surveillance dates indicated that the residence was occupied.

25 Defendant argues that the identification of the residential address of an Internet services
26 subscriber, whose assigned IP address was used to send or receive child pornography, does not
27 provide probable cause to search the subscriber’s residence. In rejecting a similar argument in
28 *United States v. Carter*, 549 F.Supp.2d 1257, 1267-68 (D.Nev. 2008), the undersigned quoted

1 *United States v. Perez*, 484 F.3d 735, 740-741 (5th Cir. 2007), *cert. denied* at 552 U.S. 952, 128
2 S.Ct. 405 (2007), as follows:

3 In this case it is clear that there was a substantial basis to conclude
4 that evidence of criminal activity would be found at 7608 Scenic
5 Brook Drive. The affidavit presented to the magistrate included the
6 information that the child pornography viewed by the witness in New
7 York had been transmitted over the IP address 24.27.21.6, and that
8 this IP address was assigned to Javier Perez, residing at 7608 Scenic
9 Brook Drive, Austin, Texas 78736. Perez argues that the association
10 of an IP address with a physical address does not give rise to probable
11 cause to search that address. He argues that if he “used an unsecure
12 wireless connection, then neighbors would have been able to easily
13 use [Perez’s] internet access to make the transmissions.” But though it
14 was possible that the transmissions originated outside of the residence
15 to which the IP address was assigned, it remained likely that the
16 source of the transmissions was inside that residence. *See United*
17 *States v. Grant*, 218 F.3d 72, 73 (1st Cir. 2000) (stating that “even
18 discounting for the possibility that an individual other than
19 [defendant] may have been using his account, there was a *fair*
20 *probability* that [defendant] was the user and that evidence of the
21 user’s illegal activities would be found in [defendant’s] home”)
22 (emphasis in original). “[P]robable cause does not require proof
23 beyond a reasonable doubt.” Brown, 941 F.2d at 1302.

24 Perez also argues that evidence that illicit transmissions were made
25 does not give rise to probable cause that physical evidence would be
26 located at the residence. However, the New York witness stated that
27 the images she observed appeared to be videos played on a television
28 screen transmitted via a web cam. There was therefore a basis to
believe that the suspect would have such videos in his residence.
Moreover, Britt stated in his affidavit that, in his experience, persons
interested in child pornography typically retain numerous images of
child pornography as well as “material documenting the arrangements,
the introduction, and tasks to consummate the acquisition of child
pornography.” Based on this information, there was probable cause to
believe that physical evidence of violations of the child pornography
laws would be located at 7608 Scenic Brook Drive.

21 In *Chism v. Washington State*, 661 F.3d 380, 390-91 (9th Cir. 2011), the Ninth Circuit
22 further comments as follows:

23 We have explained that a computer that is connected to the internet
24 can be *uniquely* identified by its IP number, much like a land-line
25 phone can be uniquely identified by its phone number. *See Forrester*,
26 512 F.3d at 510 n. 5. Moreover, we have repeatedly recognized the
27 utility of using IP address information to investigate child
28 pornography offenders. *See United States v. Craighead*, 539 F.3d
1073, 1080–81 (9th Cir. 2008) (holding that probable cause existed
where the IP address from which child pornographic images were
shared was traced to the defendant); *United States v. Hay*, 231 F.3d
630, 634–35 (9th Cir. 2000) (holding that an affidavit demonstrated
probable cause where the agent carefully detailed how the IP address

1 associated with the child pornographic images was connected to the
2 defendant). Our sister circuits take the same approach. *See, e.g.,*
3 *United States v. Vosburgh*, 602 F.3d 512, 526–27(3d Cir. 2010)
4 (“[S]everal Courts of Appeals have held that evidence that the user of
5 a computer employing a particular IP address possessed or transmitted
6 child pornography can support a search warrant for the physical
7 premises linked to that IP address.”) (footnote omitted); *United States*
8 *v. Stults*, 575 F.3d 834, 843–44 (8th Cir. 2009); *United States v.*
9 *Perrine*, 518 F.3d 1196, 1205–06 (10th Cir. 2008); *United States v.*
10 *Perez*, 484 F.3d 735, 738–40 (5th Cir. 2007); *United States v. Wagers*,
11 452 F.3d 534, 539 (6th Cir. 2006); *Hay*, 231 F.3d at 635–36; *see also*
12 *United States v. Bynum*, 604 F.3d 161, 165 (4th Cir. 2010).

13 Of course, if law enforcement agents possess other information that undermines the
14 connection between an IP address and the residential or business address associated with the internet
15 subscriber to which the IP address is assigned, then probable cause to search may be eliminated.
16 *See Chism v. Washington State, supra*. No such information has been presented in this case.

17 Probable cause is further strengthened by the nature of the conduct described in Agent
18 Hedges’ affidavit. In *United States v. Schesso*, 730 F.3d 1040, 1045-46 (9th Cir. 2013), the court
19 upheld a search warrant that was based on an affidavit substantially similar to the one in this case.
20 The affidavit identified the IP address of a computer that had been used to upload and distribute
21 child pornography on a peer-to-peer file sharing network. The IP address was assigned to the
22 defendant and on that basis the state judge issued a warrant to search his residence for child
23 pornography. In holding that the warrant was supported by probable cause, the court stated:

24 Schesso did not merely possess a commercial child pornography
25 video, which might have resulted from a onetime accidental download
26 or inadvertent receipt. Key to the probable cause analysis is the
27 evidence that Schesso took affirmative steps of uploading and
28 distributing the video on a network designed for sharing and trading.
As the affidavit explained, peer-to-peer file sharing networks are
“frequently used to trade digital files of child pornography,” “often
provide enhanced capabilities to reward those who share files by
providing reduced waiting periods, higher user ratings, or other
benefits,” and sometimes do not allow users to download files at all
unless they also share files. It is hardly a leap to infer that Schesso
either had other files to share or that he used the network to download
files.

29 It is not fatal to the finding of probable cause that Agent Hedges’ affidavit did not identify
30 Defendant Askren as a suspect. At the time the search warrant was issued, Defendant Askren was
31 presumably unknown to law enforcement. Likewise, the only basis to connect CS to the child

1 pornography images was that the IP address assigned to him had been used to make the images
 2 available for downloading. The affidavit, however, provided probable cause to search the premises
 3 at 514 Crimson View Place for evidence of child pornography. As events unfolded, the agents
 4 determined that CS was not responsible for placing the child pornography images on the ARES P2P
 5 network. Child pornography images were instead allegedly found on Defendant's computer which
 6 used CS's internet connection and assigned IP address. If the agents had discovered that someone
 7 outside the residence had used IP address 68.229.54.147 to make child pornography images
 8 available for downloading, this would not have established that probable cause for the search
 9 warrant was lacking. Instead, it would have simply led the criminal investigation in a new direction.

10 Defendant's argument that the information in the affidavit was stale is without merit.
 11 "Information underlying a warrant is not stale 'if there is sufficient basis to believe, based on a
 12 continuing pattern or other good reasons, that the items to be seized are still on the premises.'" *United States v. Schesso*, 730 F.3d. at 1047, quoting *United States v. Lacy*, 119 F.3d 742, 745-46
 13 (9th Cir. 1997). In *Schesso*, law enforcement agents applied for the warrant to search defendant's
 14 residence approximately 20 months after law enforcement agents in Germany confirmed that a child
 15 pornography video was made available on the peer-to-peer network. *Id.*, 730 F.3d at 1043. In
 16 holding that the information was not stale, the court cited the affidavit's statement that:

18 [I]ndividuals who possess, distribute, or trade in child pornography
 19 "rarely, if ever, dispose of sexually explicit images of children"
 20 because these images are treated as "prized possessions." In light of
 21 the "nature of the criminal activity and property sought" and the
 22 reasonable inference that Schesso fit the profile of a collector, the
 23 state court judge had ample reason to believe that the eDonkey video
 24 or other digital child pornography files would be present at Schesso's
 25 residence a mere 20 months after the eDonkey incident. *Id.* at 745
 26 (citation omitted); see also *United States v. Allen*, 625 F.3d 830, 842-
 43 (5th Cir. 2010) (holding that an 18-month delay between when
 defendant sent child pornography images through a peer-to-peer
 networking site and issuance of a search warrant did not render the
 information stale); *United States v. Morales-Aldahondo*, 524 F.3d
 115, 117-19 (1st Cir. 2008) (concluding that the passage of over three
 years since the acquisition of information that defendant's brother,
 who shared defendant's residence, had purchased access to various
 child pornography websites, did not render that information stale.).

27 730 F.3d at 1047.

28 ...

1 Agent Hedges' affidavit also contained "boilerplate" statements about the characteristics of
2 people who produce, trade, distribute, or possess images of child pornography, including that such
3 individuals "rarely, if ever, dispose of sexually explicit images of minors because the images are
4 treated as prized possessions." *Affidavit*, ¶12.c. The, then unidentified, individual who uploaded
5 and placed the images of child pornography on the ARES P2P network fit the characteristics of
6 child pornography collectors or distributors described in the affidavit. Given the relatively very
7 short passage of time, approximately 2 months, between the date the images were made available
8 for downloading and the date the agents applied for the warrant, there is no basis for concluding that
9 the information was stale.

10 Because the search warrant was supported by probable cause and the information was not
11 stale, it is not necessary to decide whether the good faith exception applies. If the Court was
12 required to reach that issue, however, it would hold that the agents had objectively reasonable
13 grounds to rely on the validity of the warrant. *See United States v. Underwood*, 725 F.3d at 1085,
14 citing *United States v. Leon*, 468 U.S. 897, 922, 104 S.Ct. 3405, (1984). To determine whether the
15 officer acted in objectively reasonable reliance, all of the circumstances relating to the issuance of
16 the warrant may be considered. *Id.* The Supreme Court has identified four situations that *per se* fail
17 to satisfy the good faith exception: (1) where the affiant recklessly or knowingly placed false
18 information in the affidavit that misled the issuing judge; (2) where the judge wholly abandons his
19 or her judicial role; (3) where the affidavit is so lacking in indicia of probable cause as to render
20 official belief in its existence entirely unreasonable; and (4) where the warrant is so facially
21 deficient in failing to particularize the place to be searched or the things to be seized that the
22 executing officers cannot presume it to be valid. *Id.* None of these situations apply in this case. A
23 conclusion that the warrant was not supported by probable cause would, at most, be a borderline
24 finding and would not support a conclusion that the issuing magistrate judge "wholly abandoned"
25 his judicial role or that the affidavit was so lacking in indicia of probable cause as to render official
26 belief in its existence entirely unreasonable.

27 ...

28 ...

CONCLUSION

The affidavit of Agent Hedges provided probable cause for the search of the premises at 514 Crimson View Place, Las Vegas, Nevada, 89144, including any computers found therein, for evidence of child pornography. The information contained in the affidavit was not stale.

Accordingly,


RECOMMENDATION

IT IS RECOMMENDED that Defendant's Motion to Suppress Evidence (#16) be **denied**.

NOTICE

Pursuant to Local Rule IB 3-2, any objection to this Finding and Recommendation must be in writing and filed with the Clerk of the Court within fourteen (14) days. The Supreme Court has held that the courts of appeal may determine that an appeal has been waived due to the failure to file objections within the specified time. *Thomas v. Arn*, 474 U.S. 140, 142 (1985). This circuit has also held that (1) failure to file objections within the specified time and (2) failure to properly address and brief the objectionable issues waives the right to appeal the District Court's order and/or appeal factual issues from the order of the District Court. *Martinez v. Ylst*, 951 F.2d 1153, 1157 (9th Cir. 1991); *Britt v. Simi Valley United Sch. Dist.*, 708 F.2d 452, 454 (9th Cir. 1983).

DATED this 5th day of October, 2015.



GEORGE FOLEY, JR.
United States Magistrate Judge